Fabric OS

Upgrade Guide

Supporting Fabric OS v7.4.0

BROCADE®

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier font`	Identifies CLI output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.

Convention	Description
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ x | y | z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
	In Fibre Channel products, square brackets may be used instead for this purpose.
x | y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

• OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
• Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this list identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Fabric OS 7.4.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Fabric OS.

Brocade Gen 4 platform (8-Gpbs) fixed-port switches

- Brocade 300 switch
- Brocade 5100 switch
- Brocade 5300 switch
- Brocade 5410 blade server SAN I/O module
- Brocade 5424 blade server SAN I/O module
- Brocade 5430 blade server SAN I/O module
- Brocade 5431 blade server SAN I/O module
- Brocade 5432 blade server SAN I/O module
- Brocade 5450 blade server SAN I/O module
- Brocade 5460 blade server SAN I/O module
- Brocade 5470 blade server SAN I/O module
- Brocade 5480 blade server SAN I/O module
- Brocade NC-5480 blade server SAN I/O module
- Brocade 7800 extension switch
- Brocade VA-40FC switch
- Brocade Encryption Switch

Brocade Gen 5 platform (16-Gbps) fixed-port switches

- Brocade 6505 switch
- Brocade M6505 Blade Server SAN I/O Module
- Brocade 6510 switch
- Brocade 6520 switch
- Brocade 6547 blade server SAN I/O module
- Brocade 6548 blade server SAN I/O module
- Brocade 7840 extension switch

Brocade Gen 4 platform (8-Gpbs) DCX Backbone family

- Brocade DCX
- Brocade DCX-4S

Brocade Gen 5 platform (16-Gbps) DCX Backbone family

- Brocade DCX 8510-4
- Brocade DCX 8510-8

Supported upgrade paths

The following table gives you details on supported upgrade paths and steps to upgrade through multiple versions of Fabric OS. For specific Fabric OS builds, refer to the *Fabric OS Release Notes* for that build of Fabric OS. For upgrading to other versions of Fabric OS, refer to the *Fabric OS Upgrade Guide* for the version of Fabric OS you want to upgrade to.

TABLE 1   Supported upgrade paths to Fabric OS 7.4.0

Upgrading from Fabric OS version	Upgrade Procedure
7.1.x	Direct upgrade is not supported. Upgrade to Fabric OS 7.2.x or to 7.3.0, and then to 7.4.0.
7.2.x	Use **firmwaredownload -s** to upgrade.
7.3.x	Nondisruptive upgrade.

Upgrade and downgrade considerations

Firmware upgrade and downgrade considerations for MAPS

The following firmware upgrade and downgrade considerations apply to the Monitoring and Alerting Policy Suite (MAPS) in this version of Fabric OS.

Firmware upgrade considerations

When upgrading to Fabric OS 7.4.0, there are four main scenarios:

*   Upgrading if Fabric Watch is installed but not enabled (activated) before the upgrade to Fabric OS 7.4.0.
*   Upgrading if Fabric Watch is installed and enabled before the upgrade to Fabric OS 7.4.0.
*   Upgrading if MAPS was installed before the upgrade to Fabric OS 7.4.0, but not enabled.
*   Upgrading if MAPS was installed before the upgrade to Fabric OS 7.4.0, and is enabled.

Each of these scenarios is discussed in the following sections. In addition, MAPS Fabric Performance Impact monitoring and the legacy bottleneck monitoring feature are mutually exclusive. If the legacy bottleneck monitoring feature was enabled before the upgrade, MAPS will not monitor fabric performance.

Upgrading if Fabric Watch is installed but not enabled

If Fabric Watch is installed on the switch but is not enabled at the time of the upgrade, then MAPS is installed and will monitor the fabric using the policy named "dflt_base_policy" which has the basic monitoring capabilities and will not permit you to migrate any custom Fabric Watch thresholds as part of the upgrade.

NOTE
If the Fabric Vision license is not active before you upgrade, then you cannot enable any policies and MAPS will monitor the fabric using only the basic monitoring capabilities until the Fabric Vision license is installed.

Upgrading if Fabric Watch was installed and is enabled

If Fabric Watch is installed on the switch and is enabled, then MAPS is installed with the basic monitoring capabilities, you can migrate any existing Fabric Watch thresholds as part of the change to MAPS.

Upgrading if MAPS was installed, but not enabled

If MAPS is installed on the switch but is not enabled at the time the firmware is upgraded, after the upgrade MAPS will be enabled either with the active policy named in the configuration, or if there is no active policy named, then using the default conservative policy "dft_conservative_policy". If MAPS was licensed but not enabled, you can re-enable MAPS with one of the default policies or a converted Fabric Watch policy (if Fabric Watch was licensed before upgrade) based on the Fabric Watch custom thresholds that have been converted to MAPS policies before the upgrade.

If MAPS gets enabled implicitly (without the Fabric Vision license), then any existing user-defined configurations are not initialized. After installing the Fabric Vision license, you can use one of the following setups to enable MAPS with a user-defined configuration:

- Enable MAPS using a different policy in all logical switch contexts.
- Enable MAPS by downloading a user-defined policy containing user-defined configurations.

Upgrading if MAPS was installed and is enabled

If MAPS is installed and enabled on the switch, then MAPS will continue to monitor the fabric afterwards with no change in operation. MAPS will be enabled with the same active policy that was previously in force on each logical switch and will continue to monitor the fabric based on that policy.

Upgrading firmware on Fabric Watch-licensed switches

On switches that have Fabric Watch licensed and are explicitly using Fabric Watch monitoring, upgrading to Fabric OS 7.4.0 is possible with or without migrating to MAPS. However, you must migrate to MAPS prior to upgrading in order to use any custom Fabric Watch threshold configurations, and to continue to be able use the monitoring service non-disruptively after the upgrade.

ATTENTION
Upgrading without converting Fabric Watch configurations to MAPS custom policies will result in the loss of any custom threshold configurations.

To migrate from Fabric Watch thresholds to MAPS policies, complete the following steps before upgrading to Fabric OS 7.4.0.

NOTE
Without installing the Fabric Vision license, neither converting to MAPS custom policies nor migrating to MAPS is allowed.

---

1. Enter **licenseshow** to check if the Fabric Vision license or Fabric Watch plus Advanced Performance Management (APM) licenses are available.

   - If only the Fabric Watch license is available, obtain and install an APM license.
   - If only APM license available, obtain and install a Fabric Watch license.
   - If neither is available, obtain and install a Fabric Vision license.

2. Convert Fabric Watch configurations to MAPS custom policies using the **mapsconfig --fwconvert** command.

3. Enable MAPS with one of the custom policies or default policies available using the **mapsconfig --enablemaps -policy** *policy_name* command.

The following example displays the available licences (in this case, there is a Fabric Vision license installed) and enables the "my_custom_FW_threshold" policy.

```
switch:admin> licenseshow
pSD43LDSQpFYB9Qg44ttRfN3JGXrtyYAB89Gp:
    Fabric Vision license
switch:admin> mapsconfig --enablemaps -policy my_custom_FW_threshold
```

Firmware downgrade considerations

There are three primary downgrade scenarios from Fabric OS 7.4.0 for MAPS.

• If you are downgrading from Fabric OS 7.4.0 and do not have an active Fabric Vision license, you will still have the options to use Fabric Watch or activate a license for the previous version of MAPS (if you have one) after the downgrade.

• If you are downgrading from Fabric OS 7.4.0 and have an active Fabric Vision license, when you downgrade to Fabric OS 7.3.x or 7.2.x, Fabric Watch will not be available, but you can still use MAPS at the earlier functionality level. In this case, the Fabric Watch customer thresholds are available.

• If you are downgrading from Fabric OS 7.4.0 and have an active Fabric Vision license, when you downgrade to Fabric OS 7.1.x or earlier, Fabric Watch will be available (it will require you to activate the license for it), but MAPS will not be available.

When downgrading from Fabric OS 7.4.0 to a previous version of the operating system, the following MAPS-related behaviors should be expected:

• If Fabric Watch was licensed before upgrading to Fabric OS 7.4.0, downgrading to Fabric OS 7.1.x or earlier recovers all the Fabric Watch custom configurations. If Fabric Watch was not licensed before the upgrade, then downgrading to 7.1.x or earlier means that only the non-licensed Fabric Watch monitors are restored.

• When an active Control Processor (CP) is running Fabric OS 7.2.x or later with MAPS disabled, and the standby CP has an earlier version of Fabric OS, High Availability will be synchronized, but MAPS will not be allowed to be enabled until the firmware on the standby device is changed to the matching version.

• When an active CP is running Fabric OS 7.4.0, 7.3.x, or 7.2.x and MAPS is enabled, but the standby CP is running Fabric OS 7.1.0 or earlier, then High Availability will not be synchronized until the standby CP is upgraded to Fabric OS a version of Fabric OS that matches the one on the active CP.

• On Backbone platforms that have a single CP, there is no change in behavior when downgrading to an earlier version of Fabric OS.

• Downgrading to previous versions of Fabric OS will fail if some features are not supported in the earlier firmware, and their loss could impact MAPS functionality. In this case, MAPS provides instructions on how to disable these features before firmware downgrade. An example of this is if either MAPS actions or rules include Fabric Performance Impact monitoring or port decommissioning.

The following is a list of the rules that will be affected by a downgrade from Fabric OS 7.4.0:

-      Any rules triggered by DEV_LATENCY_IMPACT with the SDDQ action.
-      Any rule that has the action SDDQ configured or if this action is enabled globally, downgrading to any version of Fabric OS that does not support the SDDQ action is blocked.
-      Any rule triggered by DEV_LATENCY_IMPACT with the FPI state IO_LATENCY_CLEAR.
-      Any rule that has the action FMS.
-      Any rule that has the action TOGGLE.

- Any rule that has the quiet time (QT) option set.
- Any rules that operate on the predefined groups ALL_CIRCUIT_HIGH_QOS, ALL_CIRCUIT_MED_QOS, ALL_CIRCUIT_LOW_QOS, and ALL_CIRCUIT_F_QOS.
- Downgrading to versions of Fabric OS prior to version 7.4.0 will trigger a warning message if any feature is not supported in the earlier firmware and keeping the feature configuration has no impact. In this case, the downgrade will not be blocked; however, MAPS will display a warning message similar to the following:
  ```
  WARNING: <A>, <B>, <C> feature(s) is/are enabled. These features are not
  available in FOS <a.b.c> release.
  Do you want to continue?
  ```
  Examples of this condition include MAPS having any user-created rules pertaining to monitoring the following: IO_LATENCY_CLEAR, ALL_CIRCUIT_HIGH_QOS, ALL_CIRCUIT_MED_QOS, ALL_CIRCUIT_LOW_QOS, ALL_CIRCUIT_F_QOS, DEV_NPIV_LOGINS, or QT.
- Downgrading to versions of Fabric OS prior to version 7.3.0 is not allowed if the MAPS Fabric Performance Impact monitoring feature is enabled. You must disable FPI using the **mapsconfig – disableFPImon** command before starting the firmware downgrade.
- Downgrading is not allowed if automatic VC quarantining has been enabled and there are slow-drain isolations already performed. The isolated slow-drain flows need to be restored to their original virtual circuits before proceeding with the downgrade because the commands to restore them will not be available in the downgraded firmware version.
- Downgrading is not allowed if there is any quarantined port in the logical group ALL_QUARANTINED_PORTS. Before you can downgrade the switch firmware, you must clear the ports from the quarantined state using the **sddquarantine --clear** *slot/port* or **all** command.

NOTE
There may be other factors affecting downgrading the firmware version; these are only the ones that MAPS affects or is affected by.

Firmware upgrade and downgrade considerations for Flow Vision

The following sections describe restrictions and considerations that apply to upgrading or downgrading the firmware on a switch with Flow Vision installed. Both user-defined and system-defined flows support the configuration upload and download procedures.

Flow Vision functionality will not be affected if a switch running Fabric OS 7.4.0 is connected to a switch running Fabric OS 7.2.x or later. Connecting to a switch running any version of Fabric OS earlier than 7.2.0 will disable Flow Vision.

Configuration file upload and download considerations

The following points should be considered when uploading or downloading configuration files.

- When uploading a configuration file created in an earlier version of Fabric OS to Fabric OS 7.4.0, the Fabric OS 7.4.0 predefined flows are automatically created, but remain deactivated.
- When downloading a configuration file created in Fabric OS 7.4.0 to switches running Fabric OS 7.3.x or 7.2.x, the Fabric OS 7.4.0 predefined flows are included, but are deactivated. After downloading, these flows will not be replayed from the flow configuration. Flow definitions for features introduced Fabric OS 7.4.0 are ignored.

Firmware upgrade and downgrade considerations for Peer Zoning

When a switch containing Peer Zones is upgraded to Fabric OS 7.4.0, Peer Zoning connectivity rules are enforced on the devices attached to the upgraded switch. If the device is a member of a Peer Zone, the upgrade can cause disruption.

When a switch containing Peer Zones is downgraded from Fabric OS 7.4.0 to an earlier version, the Peer Zones are treated as regular zones and the zones follow the regular zoning connectivity rules.

All devices in the Peer Zone must be attached to switches running Fabric OS 7.4.0 or later, for the Peer Zoning connectivity rules to be applied. If any device that is part of the Peer Zone is attached to a switch running an earlier version of Fabric OS, the Peer Zone will be treated as a regular zone.

After downgrading to an earlier version of Fabric OS, Peer Zoning connectivity rules remain on the switch until a port of the Peer Zone device is toggled or a new zoning configuration is committed. In such a case, the regular zoning rules apply to the Peer Zones.

Installing and Maintaining Firmware

Firmware download process overview

Fabric OS 7.4.0 provides nondisruptive firmware installation.

This chapter refers to the following specific types of blades inserted into the Brocade DCX, and DCX 8510 Backbone families:

- FC blades or port blades that contain only Fibre Channel ports; the Brocade FC8-16, FC8-32, FC8-48, and FC8-64; and the Brocade FC16-32, FC16-48, and FC16-64 blades for 16-Gbps-capable FC blades.
- AP blades contain extra processors and specialized ports: FCOE10-24, FX8-24, and FS8-18 encryption blade.
- CP blades have a control processor (CP) used to control the entire switch; CP blades can be inserted only into slots 6 and 7 on the Brocade DCX, or DCX 8510-8, and slots 4 and 5 on the Brocade DCX-4S, and DCX 8510-4.
- CR8 and CR4S-8 core blades provide ICL functionality between two Brocade DCX Backbones. CR8 blades can be inserted only into slots 5 and 8 on the Brocade DCX. CR4S-8 blades can be inserted only into slots 3 and 6 on the Brocade DCX-4S.
- CR16-4 and CR16-8 core blades provide ICL functionality between two Brocade DCX 8510. CR16-4 blades can be inserted only into slots 3 and 6 on the Brocade DCX 8510-4. CR16-8 blades can be inserted only into slots 5 and 8 on the Brocade DCX 8510-8.

NOTE
For more information on troubleshooting a firmware download, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*.

You can download Fabric OS to a Backbone, which is a chassis; and to a nonchassis-based system, also referred to as a fixed-port switch. The difference in the download process is that Backbones have two CPs and fixed-port switches have one CP. Use the **firmwareDownload** command to download the firmware from either an FTP or SSH server by using FTP, SFTP, or SCP to the switch. Or, you can use a Brocade-branded USB device.

New firmware consists of multiple files in the form of RPM packages listed in a .plist file. The .plist file contains specific firmware information (time stamp, platform code, version, and so forth) and the names of packages of the firmware to be downloaded. These packages are made available periodically to add features or to remedy defects. Contact your switch support provider to obtain information about available firmware versions.

All systems maintain two partitions (a primary and a secondary) of nonvolatile storage areas to store firmware images. The firmware download process always loads the new image into the secondary partition. It then swaps the secondary partition to be the primary and High Availability (HA) reboots (which is nondisruptive) the system. After the system boots up, the new firmware is activated. The firmware download process then copies the new image from the primary partition to the secondary partition.

In dual-CP systems, the firmware download process, by default, sequentially upgrades the firmware image on both CPs using HA failover to prevent disruption to traffic flowing through the Backbone. This operation depends on the HA status on the Backbone. If the platform does not support HA, you can still upgrade the CPs one at a time.

If you are using a Brocade DCX, or DCX 8510, Backbone family platform, with one or more AP blades: Fabric OS automatically detects mismatches between the active CP firmware and the blade's firmware and triggers the autoleveling process. This autoleveling process automatically updates the blade firmware to match the active CP. At the end of the autoleveling process, the active CP and the blade run the same version of the firmware.

If the firmware download process is interrupted by an unexpected reboot, the system automatically repairs and recovers the secondary partition. You must wait for the recovery to complete before issuing another **firmwareDownload** command.

The command supports both noninteractive and interactive modes. If the **firmwareDownload** command is issued without any operands, or if there is any syntax error in the parameters, the command enters an interactive mode, in which you are prompted for input.

ATTENTION
For each switch in your fabric, complete all firmware download changes on the current switch before issuing the **firmwareDownload** command on the next switch. This process ensures nondisruption of traffic between switches in your fabric. To verify the firmware download process is complete, enter the **firmwareDownloadStatus** command on the switch, verify the process is complete, and then move to the next switch.

Considerations for FTP server credentials with special characters

FTP server credentials may include special characters that need to be handled in specified manner on the Command Line Interface (CLI).

Special characters also referred to as meta-characters, are members of an exempt set of characters, which when used in command line mode are evaluated as characters with non-literal meaning. These characters are designated to carry out a special instruction, or have an alternate meaning.

NOTE
This list is not exhaustive and alternate meaning for some characters is contextual. For more information, refer to any Linux scripting information available for general use on the internet.

A list of some of the more commonly used special characters and their alternate meaning is as follows:

- **&** is used to put a command in background/batch mode.
- **!** is used to recall the last invocation of the command matching the pattern that follows the character.
- **|** is used to pipe output to the command that follows the character.
- **;** is used to concatenate multiple bash commands.
- ***** is used to represent a wildcard character.

- **?** is used as a match for any single character in the specified position.
- **()** is used for integer expansion.
- **<>** is used for redirection. **<** represents input and **>** represents output.
- **$** is used to represent shell variable.
- **`** is used for command substitution or assign output of a command to a variable.
- **"** is used for partial quoting.
- **'** is used for full quoting.
- Space is used as a separation character.
- **#** when preceded by a space, treats all characters till the end of the corresponding line as a comment.

These special characters may be used to enhance the security of the user credentials. However, to interpret these characters properly in the CLI mode, you must follow one of the following methods:

- Escape each instance of the special character by preceding it with the escape character (\).
- Enclose the credentials containing special characters, with single quotes.

If single quotes are themselves part of the credential, precede each instance of the single quote with the escape character (\). Alternately, the string may be enclosed in double quotes if more intricate bash substitution is desired to further strengthen the security measure of the credentials.

For detailed information on using the special characters in the credentials, refer to any Linux scripting information available for general use on the internet.

You can test the representation of the credentials using the echo tests.

Examples to verify the use of special characters

To verify the use of single quote for the password aaa!01:
```
switch:admin> echo 'aaa!01'
aaa!01
```

To verify escaping ! without quotes for the password aaa!01:
```
switch:admin> echo aaa\!01
aaa!01
```

To verify using the quotes, excluding the \! for password aaa!01:
```
switch:admin> echo "aaa"\!"01"
aaa!01
```

To verify using the quotes without excluding the \! for password aaa!01, resulting in different password pattern:
```
switch:admin> "aaa\!01"
aaa\!01
```

To verify using the quotes around the \! for password aaa!01, resulting in different password pattern:
```
switch:admin> echo 'aaa!01'
aaa!01
```

Upgrading and downgrading firmware

Upgrading means installing a newer version of firmware. *Downgrading* means installing an older version of firmware.

In most cases, you will be *upgrading* firmware; that is, installing a newer firmware version than the one you are currently running. However, some circumstances may require installing an older version; that is, *downgrading* the firmware. The procedures in this section assume that you are upgrading firmware, but they work for downgrading as well, provided the old and new firmware versions are compatible. Always reference the latest release notes for updates that may exist regarding downgrades under particular circumstances.

During the firmware upgrade, the configuration file uploaded from firmware versions Fabric OS 7.2.x and Fabric OS 7.3.x is allowed to download to Fabric OS v7.4.0.

During the firmware downgrade, the configuration file uploaded from v7.4.0 is allowed to download to previous firmware versions Fabric OS 7.2.x and Fabric OS 7.3.x.

For details on Administrative Domains and the firmware download process, refer to the *Managing Administrative Domains* chapter in the *Fabric OS Administrator's Guide* for more information.

For details about testing and restoring firmware, refer to

Passwordless firmware download

You can download firmware without a password using the **sshutil** command for public key authentication when SSH is selected. The switch must be configured to install the private key, and then you must export the public key to the remote host. Before running the **firmwareDownload** command, you must first configure the SSH protocol to permit passwordless logins for outgoing authentication as described in the *Configuring outgoing SSH authentication* section in the *Fabric OS Administrator's Guide*.

Staging the firmware download

The firmware that has been downloaded to the secondary partition using the **firmwareDownload –r** command can be activated later using the **firmwareActivate** command. You can also download the firmware with local mode (current CP) using the **firmwareDownload –lr** command and activate it later using the **firmwareActivate –l** command. After the firmware is downloaded, it is incomplete until the new firmware is activated. Perform any configuration changes before activating the new firmware. If the switch reboots or panics, the firmware does not get affected as it is downloaded to the secondary partition. The **firmwareRestore** or **firmwareCommit** does not start until the firmware is activated. The **firmwareActivate** command can be used in both single-CP and dual-CP environments.

1. Download the firmware with any of the previously mentioned options.
2. Enter the **firmwareShow** command to know the status of the download.

```
sw0:FID128:admin> firmwareshow
Slot Name        Appl    Primary/Secondary Versions                 Status
-------------------------------------------------------------------------
  4  CP0         FOS     v7.4.0                                      ACTIVE *
                         v7.4.0
  5  CP1         FOS     v7.4.0                                      STANDBY
                         v7.4.0
 *  Local CP

Firmware download completed. Please activate using firmwareactivate.
```

3. Activate the firmware using the **firmwareActivate** command.

```
sw0:FID128:admin>firmwareactivate
This command will activate the firmware on the secondary partition
but will require that existing telnet, secure telnet or SSH sessions to be
restarted.

Do you want to continue (Y/N) [Y]:
```

Considerations for FICON CUP environments

To prevent channel errors during nondisruptive firmware installation, the switch CUP port must be taken offline from all host systems.

HA sync state

High Availability (HA) synchronization occurs when two CPs in a Backbone are synchronized. This state provides redundancy and a nondisruptive firmware download. In order for a firmware download to successfully occur, the two CPs in a Backbone must be in sync.

If the CPs have mixed versions when you enter the **firmwareDownload** command, the CPs may not be in HA sync. In this case, you must enter the **firmwareDownload -s** command first to upgrade or downgrade the standby CP to the same level as the active CP, and then upgrade the CPs to the desired version of firmware. You can also sync the firmware on the active CP to the standby CP using the **firmwaresync** command.

NOTE
Do not run mixed firmware levels on CPs.

Table 2 shows the sync state of a Backbone that has different Fabric OS versions installed on the active and standby CPs. Use the table to determine if you need to use the **firmwareDownload -s** command.

TABLE 2   Backbone HA sync states

Active CP Fabric OS version	Standby CP Fabric OS version	HA sync state	Remedy
v7.0.0	v7.0.0	In sync	N/A
v7.0.0	v7.1.0	In sync	N/A
v7.0.0	v7.2.0	Not in sync	Upgrade Active CP to v7.2.0.
v7.1.0	v7.0.0	In sync	N/A
v7.1.0	v7.1.0	In sync	N/A
v7.1.0	v7.2.0	In sync	N/A
v7.1.0	v7.3.0	Not in sync	Run **firmwareDownload -s** on the active CP to upgrade it to v7.3.0
v7.1.0	v7.4.0	Not in sync	Run **firmwareDownload -s** on the active CP to upgrade it to v7.4.0
v7.2.0	v7.1.0	In sync	N/A
v7.2.0	v7.2.0	In sync	N/A
v7.2.0	v7.3.0	In sync	N/A

TABLE 2 Backbone HA sync states (Continued)

Active CP Fabric OS version	Standby CP Fabric OS version	HA sync state	Remedy
v7.2.0	v7.4.0	In sync	N/A
v7.3.0	v7.1.0	Not in sync	Run **firmwareDownload -s** on the standby CP to upgrade it to v7.3.0
v7.3.0	v7.2.0	In sync	N/A
v7.3.0	v7.3.0	In sync	N/A
v7.3.0	v7.4.0	In sync	N/A
v7.4.0	v7.1.0	Not in sync	Run **firmwareDownload -s** on the active CP to upgrade it to v7.4.0
v7.4.0	v7.2.0	In sync	N/A
v7.4.0	v7.3.0	In sync	N/A
v7.4.0	v7.4.0	In sync	N/A
v7.4.0	vx.x.x	In sync	N/A

NOTE
You can use the **firmwareCleanInstall** command in cases where you need to return to the defaults and multiple levels of Fabric OS versions need to be skipped. This command does not require HA in sync. The least or minimum version that can be downloaded using the **firmwareCleanInstall** command is Fabric OS 6.4.0. Starting with Fabric OS 7.4.0, the **firmwareCleanInstall** command is available to both root and admin users.

ATTENTION
When you run the **firmwareCleanInstall** command, the storage is reformatted and all data and code including the configuration file in the CP are removed. Only the configuration storage in the WWN card, such as IP addresses, is preserved. Do not run the **firmwareCleanInstall** command on both CPs at the same time as the CPs reboot independently of each other.

NOTE
During nondisruptive firmware download or disruptive firmware download with the **commit** option, firmware commit should start as a part of firmware download after the HA state gets in sync. Firmware commit can also be triggered when any failure happens, such as sync failure and standby reboot failure during firmware download before the HA state gets in sync.

Displaying the HA redundancy status

To display the switch uptime and CP blades redundancy settings, use the **haRedundancy --show** command.

The **haRedundancy** command displays the following information:

- Current active session details.

    - HA synchronization status.
    - Active slot state: CP ID, (local/remote CP), recovery type.
    - Standby slot state: CP ID, (local/remote CP).
    - Start time: The starting time of all service becoming in sync state. Displayed when HA is in sync state.

- Previous active session

    - Active slot state: CP ID, recovery type.
    - Standby slot state: CP ID
    - Start time: Starting time of previous active session when all service instances became in sync.
    - End time: Ending time of previous active session caused by expected or unexpected recovery.

- System uptime

    The starting time since system services has been running. It will not change unless you power cycle the system or reset both CPs at the same time.

For an example, refer to the following output from a DCX 8510-8 chassis with a healthy standby CP blade.

```
sw0:FID128:admin> haredundancy --show
=== HA Redundancy Statistics ===
HA State synchronized
Current Active Session:
Active Slot = CP0 (Local), Expected Recovered
Standby Slot = CP1 (Remote)
Start Time: 17:55:33 UTC Fri Jan 03 2014

Previous Active Session:
Active Slot = CP1, Expected Recovered
Standby Slot = CP0
Start Time: 17:49:46 UTC Fri Jan 03 2014
End Time: 17:54:10 UTC Fri Jan 03 2014

System Uptime: 17:42:11 UTC Fri Jan 03 2014
```

Enabling automatic firmware synchronization from active CP to the standby CP

You can enable automatic firmware synchronization from the active CP blade to the standby CP blade if the following requirements are met:

- The standby CP must be hot-plugged.
- If the firmware version in the active CP is Fabric OS 7.4.0 or later, the firmware on the standby CP can be any older or newer version.
- The firmware upgrade process in the standby CP must not be currently running or already initiated.

To enable firmware auto-synch from active CP to standby CP, use the **configureChassis** command.

```
sw0:FID128:admin> configurechassis

Configure...

  cfgload attributes (yes, y, no, n): [no] y

    Enforce secure config Upload/Download (yes, y, no, n): [yes]
    Enforce signature validation for firmware (yes, y, no, n): [yes]
    Add Suffix to the uploaded file name (yes, y, no, n): [yes]
    Do you want to enable auto firmwaresync (yes, y, no, n): [yes] y
```

The firmware is synced from the primary partition of active CP to the secondary partition of standby CP. After the sync is completed, the standby CP reboots with auto-commit enabled. The standby CP does not require external Ethernet connection as the synching of firmware takes place through the backplane connection between active and standby CP blades. This configuration setting is not included in the **configUpload** or **configDownload** process.

Manually synchronizing the firmware from the active CP to the standby CP

You can use the **firmwareSync** command to synchronize the firmware from the active CP to the standby CP. If you have Fabric OS 7.4.0 or later in the active CP, the standby CP firmware version can be any older or newer version.

```
sw0:FID128:admin> firmwaresync

This command will copy the firmware on the active CP blade to the
Standby CP blade but will require that existing telnet, secure telnet or
SSH sessions to the standby CP blade to be restarted.

This command may take up to 10 minutes.

Do you want to continue (Y/N) [Y]: y

Firmwaresync has started.............................
.
.....Firmwaresync has been completed successfully.
2014/05/06-03:42:21, [SULB-1053], 1461, SLOT 5 | CHASSIS, INFO, Brocade-DCX,
Firmware sync to the secondary partition of standby CP has been completed.
It will perform auto-reboot followed by auto-commit.
```

Preparing for a Firmware Download

Prerequisites

Before executing a firmware download, it is recommended that you perform the tasks listed in this section. In the unlikely event of a failure or timeout, these preparatory tasks enable you to provide your switch support provider the information required to troubleshoot the firmware download.

It is recommended that you use the **configUpload** command to back up the current configuration before you download firmware to a switch. Refer to the *Configuration file backup* section in the *Fabric OS Administrator's Guide* for details.

1. Read the release notes for the new firmware to find out if there are any updates related to the firmware download process.

2. Connect to the switch and log in using an account with admin permissions. Enter the **firmwareShow** command to verify the current version of Fabric OS.

   Brocade does not support non-disruptive upgrades from more than two previous releases. Non-disruptive upgrade is supported on Fabric OS 7.2.x and Fabric OS 7.3.x to Fabric OS 7.4.x.

   Disruptive upgrade from Fabric OS 7.1.x to Fabric OS 7.4.x is supported.

3. Use the **configUpload** command prior to the firmware download. Save the configuration file on your FTP or SSH server or USB memory device on supported platforms. Refer to Considerations for FTP server credentials with special characters on page 18 for information on use of special characters.

4. *Optional:* For additional support, connect the switch to a computer with a serial console cable. Ensure that all serial consoles (both CPs for Backbones) and any open network connection sessions, such as Telnet, are logged and included with any trouble reports.

5. Connect to the switch and log in using an account with admin permissions. Enter the **supportSave** command to retrieve all current core files prior to executing the firmware download. This information helps to troubleshoot the firmware download process if a problem is encountered.

6. *Optional:* Enter the **errClear** command to erase all existing messages in addition to internal messages.

Obtaining and decompressing firmware

Firmware upgrades are available for customers with support service contracts and for partners on the Brocade website at http://www.brocade.com .

You must decompress the firmware *before* you can use the **firmwareDownload** command to update the firmware on your equipment. Use the UNIX tar command for .tar files, the gunzip command for all .gz files, or a Windows unzip program for all .zip files

When you unpack the downloaded firmware, it expands into a directory that is named according to the version of Fabric OS it contains. For example, when you download and unzip v7.4.0.zip, it expands into a directory called v7.4.0. When you issue the **firmwareDownload** command, there is an automatic search for the correct package file type associated with the switch. Specify only the path up to and including the v7.4.0 directory.

Connected switches

Before you upgrade the firmware on your switch, you must check the connected switches to ensure compatibility and that any older versions are supported. Refer to the Fabric OS Compatibility section of the *Brocade Fabric OS Release Notes* for the recommended firmware version.

If fixed-port switches are adjacent and you start firmware downloads on them at the same time, there may be traffic disruption.

To determine if you need to upgrade switches connected to the switch you are upgrading, use the following procedure on each connected switch to display firmware information and build dates.

Finding the switch firmware version

1. Connect to the switch and log in using an account with admin permissions.
2. Enter the **version** command.

   The following information is displayed:

   - **Kernel**: Displays the version of the switch kernel operating system.
   - **Fabric OS**: Displays the version of the switch Fabric OS.
   - **Made on**: Displays the build date of the firmware running on the switch.
   - **Flash**: Displays the install date of firmware stored in nonvolatile memory.
   - **BootProm**: Displays the version of the firmware stored in the boot PROM.

Firmware Download Scenarios

Firmware download on switches

Brocade fixed-port switches maintain primary and secondary partitions for firmware. The **firmwareDownload** command defaults to an autocommit option that automatically copies the firmware from one partition to the other.

NOTE
This section only applies when upgrading from Fabric OS v7.3.x to v7.4.0, downgrading from v7.4.0 to v7.3.x, or going from v7.3.x to v7.4.x. If you are upgrading from Fabric OS v7.2.x to v7.4.0 or downgrading from v7.4.0 to v7.2.x, you must enter the **firmwareDownload -s** command as described in Testing and restoring firmware on switches on page 33.You cannot download firmware if you are going from v7.4.0 to v7.1.0 (or earlier) or from v7.1.0 (or earlier) to v7.4.0.

Do not override the autocommit option under normal circumstances; use the default. Refer to Testing and restoring firmware on Backbones on page 34 for details about overriding the autocommit option.

NOTE
A VE port on Brocade 7800 or Brocade 7840 can go down due to external events during hot code load. In such scenario, traffic is disrupted on that particular VE port. After the hot code load completes, it may be possible that such VE port comes up as G_Port and traffic may not resume. In such scenario, you need to perform explicit **portDisable** and **portEnable** on that VE port to recover.

Switch firmware download process overview

The following list describes the default behavior after you enter the **firmwareDownload** command (without options) on Brocade fixed-port switches:

• The Fabric OS downloads the firmware to the secondary partition.
• The system performs a high availability reboot (**haReboot**). After the **haReboot** , the former secondary partition is the primary partition.
• The system replicates the firmware from the primary to the secondary partition.

The upgrade process first downloads and then commits the firmware to the switch. While the upgrade is proceeding, you can start a session on the switch and use the **firmwareDownloadStatus** command to observe the upgrade progress.

> ⚠️ **CAUTION**
>
> **After you start the process, do not enter any disruptive commands (such as reboot) that interrupt the process. The entire firmware download and commit process takes approximately 17 minutes. If there is a problem, wait for the timeout (30 minutes for network problems) before issuing the firmwareDownload command again. Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider.Do not disconnect the switch from power during the process. The switch could be inoperable when rebooted.**

Upgrading firmware for Brocade fixed-port switches

1. Take the following appropriate action based on what service you are using:

   - If you are using FTP, SFTP, or SCP, verify that the FTP or SSH server is running on the host server and that you have a valid user ID and password on that server.
   - If your platform supports a USB memory device, verify that it is connected and running.

2. Obtain the firmware file from the Brocade website at http://www.brocade.com and store the file on the FTP or SSH server or the USB memory device.

3. Unpack the compressed files preserving directory structures.

   The firmware is in the form of RPM packages with names defined in a . plist file. The .plist file contains specific firmware information and the names of packages of the firmware to be downloaded.

4. Connect to the switch and log in using an account with admin permissions.

5. Issue the **firmwareShow** command to check the current firmware version on connected switches. Upgrade the firmware on the connected switches, if necessary, before proceeding with upgrading this switch.

   Refer to for details.

6. Enter the **firmwareDownload** command and respond to the prompts.

   NOTE
   If DNS is enabled and a server name instead of a server IP address is specified in the command line, **firmwareDownload** determines whether IPv4 or IPv6 should be used.To be able to mention the FTP server by name, you must enter at least one DNS server using the **dnsConfig** command.

7. At the "Do you want to continue [y/n]" prompt, enter **y** .

8. After the HA reboot, connect to the switch and log in again using an account with admin permissions.

9. Enter the **firmwareDownloadStatus** command to determine if the firmware download process has completed.

10. After the firmware commit is completed, which takes several minutes, enter the **firmwareShow** command to verify the firmware level of both partitions is the same.

   Example of an interactive firmware download

   ```
   switch:admin> firmwaredownload
   Server Name or IP Address: 10.31.2.25
   User Name: admin
   File Name: /home/SAN/fos/v7.4.0/v7.4.0
   Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 4
   Verifying if the public key authentication is available.Please wait ...
   The public key authentication is not available.
   Password:
   Server IP: 10.31.2.25, Protocol IPv4
   Checking system settings for firmwaredownload...
   ```

Firmware download on a Backbone

ATTENTION

To successfully download firmware, you must have an active Ethernet connection on each CP.

You can download firmware to a Backbone without disrupting the overall fabric if the two CP blades are installed and fully synchronized. Use the **haShow** command to verify that the CPs are synchronized prior to beginning the firmware download process. If only one CP blade is inserted, powered on, or plugged into the network, you can run **firmwareDownload -s** to upgrade the CP. If the CPs are not in sync, you can run **firmwareDownload -s** on each of the CPs to upgrade them. These operations are disruptive. If the CPs are not in sync, run the **haSyncStart** command. If the CPs are still not in sync, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*. If the troubleshooting information fails to help resolve the issue, contact your switch service provider.

During the upgrade process, the Backbone fails over to its standby CP blade and the IP address for the Backbone moves to that CP blade's Ethernet port. This may cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.

Backbone firmware download process overview

The following summary describes the default behavior of the **firmwareDownload** command (without options) on a Backbone. After you enter the **firmwareDownload** command on the active CP blade the following actions occur.

1. The standby CP blade downloads firmware.
2. The standby CP blade reboots and comes up with the new Fabric OS.
3. The active CP blade synchronizes its state with the standby CP blade.
4. The active CP blade forces a failover and reboots to become the standby CP blade.
5. The new active CP blade synchronizes its state with the new standby CP blade.
6. The new standby CP blade (the active CP blade before the failover) downloads firmware.
7. The new standby CP blade reboots and comes up with the new Fabric OS.
8. The new active CP blade synchronizes its state with the new standby CP blade.
9. The **firmwareCommit** command runs automatically on both CP blades.

CAUTION

After you start the process, do not enter any disruptive commands (such as reboot) that interrupt the process. The entire firmware download and commit process takes approximately 17 minutes. If there is a problem, wait for the timeout (30 minutes for network problems) before issuing the firmwareDownload command again. Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider.Do not disconnect the switch from power during the process. The switch could be inoperable when rebooted.

Upgrading firmware on Backbones (including blades)

There is only one chassis management IP address for the Brocade Backbones.

1. Verify that the Ethernet interfaces located on CP0 and CP1 are plugged into your network. If the switch has a BP, verify that the BP console is accessible.

2. Verify that the FTP, SFTP, or SSH server is running on the host server and that you have a user ID on that server.

3. Obtain the firmware file from the Brocade website at http://www.brocade.com and store the file on the FTP or SSH server.

4. Unpack the compressed files preserving directory structures.

   The firmware is in the form of RPM packages with names defined in a .plist file. The .plist file contains specific firmware information and the names of packages of the firmware to be downloaded.

5. Connect to the chassis IP management interface or active CP and log in using an account with admin permissions.

6. Use the **firmwareShow** command to check the current firmware version on connected switches. Upgrade the firmware, if necessary, before proceeding with upgrading this switch.

   Refer to

7. Enter the **haShow** command to confirm that the two CP blades are synchronized.

   In the following example, the active CP blade is CP0 and the standby CP blade is CP1:

   ```
   ecp:admin> hashow
   Local CP (Slot 5, CP0): Active, Warm Recovered
   Remote CP (Slot 6, CP1): Standby, Healthy
   HA enabled, Heartbeat Up, HA State synchronized
   ```

   CP blades must be synchronized and running Fabric OS v7.2.0 or later to provide a nondisruptive download. If the two CP blades are not synchronized, enter the **haSyncStart** command to synchronize them. If the CPs still are not synchronized, contact your switch service provider.

   For further troubleshooting, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*.

8. Enter the **firmwareDownload** command and respond to the interactive prompts.

9. At the "Do you want to continue [y/n]" prompt, enter **y.**

   The firmware is downloaded to one CP blade at a time, beginning with the standby CP blade. During the process, the active CP blade fails over. After the firmware is downloaded, a firmware commit starts on both CP blades. The entire firmware download and commit process takes approximately 17 minutes.

   If an AP blade is present : At the point of the failover, an *autoleveling* process is activated. Autoleveling is triggered when the active CP detects a blade that contains a different version of the firmware, regardless of which version is older. Autoleveling downloads firmware to the AP blade, swaps partitions, reboots the blade, and copies the new firmware from the primary partition to the secondary partition. If you have multiple AP blades, they are updated simultaneously; however, the downloads can occur at different rates.

   Autoleveling takes place in parallel with the firmware download being performed on the CPs, but does not impact performance. Fibre Channel traffic is not disrupted during autoleveling, but GbE traffic on AP blades may be affected. If there is an active FCIP tunnel on the FX8-24 blade, the FCIP tunnel traffic will be impacted for at least two minutes.

   ```
   ecp:admin> firmwaredownload
   Server Name or IP Address: 10.1.2.3
   User Name: userfoo
   File Name: /home/userfoo/v7.4.0
   Network Protocol (1-auto-select, 2-FTP, 3-SCP, 4-SFTP)) [1]:
   Password: <hidden>
   Checking version compatibility...
   Version compatibility check passed.
   The following AP blades are installed in the system.
   Slot Name      Versions                      Traffic Disrupted
   ------------------------------------------------------------
   2  FS8-18    v7.4.0          Encrypted Traffic
   ```

```
8  FX8-24    v7.4.0              GigE
This command will upgrade the firmware on both CPs and all AP blade(s) above.
If you want to upgrade firmware on a single CP only, please use -s option.
You may run firmwaredownloadstatus to get the status of this
command.
This command will cause a warm/non-disruptive boot on the active CP,
but will require that existing telnet, secure telnet or SSH sessions
be restarted.
Do you want to continue [Y]: y
The firmware is being downloaded to the Standby CP. It may take up to 10 minutes.
```

10. Optionally, after the failover, connect to the switch, and log in again as admin. Using a separate session to connect to the switch, enter the **firmwareDownloadStatus** command to monitor the firmware download status.

```
sw0:FID128:admin> firmwaredownloadstatus
[1]: Mon Jul 22 04:27:21 2013
Slot 7 (CP1, active): Firmware is being downloaded to the switch. This step may
take up to 30 minutes.
[2]: Mon Jul 22 04:34:58 2013
Slot 7 (CP1, active): Relocating an internal firmware image on the CP blade.
[3]: Mon Jul 22 04:35:29 2013
Slot 7 (CP1, active): The internal firmware image is relocated successfully.
[4]: Mon Jul 22 04:35:30 2013
Slot 7 (CP1, active): Firmware has been downloaded to the secondary partition of
the switch.
[5]: Mon Jul 22 04:37:24 2013
Slot 7 (CP1, standby): The firmware commit operation has started. This may take up
to 10 minutes.
[6]: Mon Jul 22 04:41:59 2013
Slot 7 (CP1, standby): The commit operation has completed successfully.
[7]: Mon Jul 22 04:41:59 2013
Slot 7 (CP1, standby): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

11. Enter the **firmwareShow** command to display the new firmware versions.

Firmware download from a USB device

NOTE

Pre-formatted USB sticks are available through technical support.

The Brocade 300, 5100, 5300, 6505, 6510, 6520, 7800, 7840, and VA-40FC switches and the Brocade DCX, DCX-4S, DCX 8510 Backbones support a firmware download from a Brocade-branded USB device attached to the switch or active CP. Before the USB device can be accessed by the **firmwareDownload** command, it must be enabled and mounted as a file system. The firmware images to be downloaded must be stored under the relative path from /usb/usbstorage/brocade/ firmware or use the absolute path in the USB file system. Multiple images can be stored under this directory. There is a firmwarekey directory where the public key signed firmware is stored.

When the **firmwareDownload** command line option, -U (uppercase), is specified, the **firmwareDownload** command downloads the specified firmware image from the USB device. When specifying a path to a firmware image in the USB device, you can only specify the relative path to / firmware or the absolute path.

NOTE

You must unmount the USB device using the **usbStorage -d** command before removing the USB device from the switch.

Enabling the USB device

1. Log in to the switch using an account assigned to the admin role.
2. Enter the **usbStorage -e** command.

Viewing the USB file system

1. Log in to the switch using an account assigned to the admin role.
2. Enter the **usbStorage -I** command.

```
BrcdDCXBB:admin> usbstorage -l
firmware\                 381MB    2015 Jan 22 15:33
  v7.4.0\                 381MB    2015 Jan 22 10:39
config\                   0B       2015 Jan 22 15:33
support\                  0B       2015 Jan 22 15:33
firmwarekey\              0B       2015 Jan 22 15:33
Available space on usbstorage 79%
```

Downloading from the USB device using the relative path

1. Log in to the switch using an account assigned to the admin role.
2. Enter the **firmwareDownload -U** command.

```
ecp:admin>firmwaredownload -U v7.4.0
```

Downloading from the USB device using the absolute path

1. Log in to the switch using an account assigned to the admin role.
2. Enter the **firmwareDownload** command with the -U operand.

```
ecp:admin>firmwaredownload -U /usb/usbstorage/brocade/firmware/v7.4.0
```

Testing and Restoring Firmware

Testing and restoring firmware on switches

Typically, users downgrade firmware after briefly evaluating a newer (or older) version and then restore the original version of the firmware. Testing a new version of firmware in this manner ensures that you do not replace existing firmware because the evaluated version occupies only one partition on the switch.

ATTENTION

When you evaluate new firmware, make sure you disable all features that are not supported by the original firmware before restoring to the original version.

Testing a different firmware version on a switch

1. Verify that the FTP, SFTP, or SSH server is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the Brocade website at http://www.brocade.com or the switch support provider and store the file on the FTP or SSH server.
3. Unpack the compressed files preserving directory structures.

   The firmware is in the form of RPM packages with names defined in a .plist file that contains specific firmware information and the names of packages of the firmware to be downloaded.
4. Connect to the switch and log in using an account with admin permissions.
5. Enter the **firmwareShow** command to view the current firmware.
6. Enter the **firmwareDownload -s** command to update the firmware, and respond to the prompts.

   Example of a firmware download to a single partition

   ```
   ecp:admin> firmwareDownload -s
   Server Name or IP Address: 10.1.2.3
   Network Protocol (1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]:
   User Name: userfoo
   File Name: /home/userfoo/v7.4.0
   Password: <hidden>
   Do Auto-Commit after Reboot [Y]: n
   Reboot system after download [N]: y
   Firmware is being downloaded to the switch. This step may take up to 30 minutes.
   Checking system settings for firmwaredownload...
   ```

   The switch performs a reboot and comes up with the new firmware to be tested. Your current switch session automatically disconnects.

ATTENTION

Downloading firmware to a switch can be disruptive to switch traffic.

---

7. Connect to the switch, log in as admin, and enter the **firmwareShow** command to confirm that the primary partition of the switch contains the new firmware.

   You are now ready to evaluate the new version of firmware.

ATTENTION

Stop! If you want to *restore* the firmware, stop here and skip ahead to step 9; otherwise, continue to step 8 to commit the firmware on the switch, which completes the firmware download operations.

---

8. Commit the firmware.

   a)   Enter the **firmwareCommit** command to update the secondary partition with new firmware. Note that it takes several minutes to complete the commit operation.

   b)   Enter the **firmwareShow** command to confirm both partitions on the switch contain the new firmware.

   ATTENTION

   Stop! If you have completed step 8, then you have committed the firmware on the switch and you have completed the firmware download procedure.

   ---

9. Restore the firmware.

   a)   Enter the **firmwareRestore** command. The switch reboots and comes up with the original firmware again.

   A firmware commit automatically begins to copy the original firmware from the primary partition to the secondary partition. At the end of the firmware commit process, both partitions have the original firmware. Note that it takes several minutes to complete the commit operation.

   b)   Wait five minutes to ensure that all processes have completed and the switch is fully up and operational.

   c)   Log in to the switch. Enter the **firmwareShow** command and verify that both partitions on the switch have the original firmware.

Testing and restoring firmware on Backbones

This procedure enables you to perform a firmware download on each CP and verify that the procedure was successful before committing to the new firmware. The old firmware is saved in the secondary partition of each CP until you enter the **firmwareCommit** command. If you decide to back out of the installation prior to the firmware commit, you can enter the **firmwareRestore** command to restore the former active Fabric OS firmware image.

The **firmwareRestore** command can only run if autocommit was disabled during the firmware download. This command cannot be used to restore SAS and SA images.

NOTE
Brocade recommends that, under normal operating conditions, you maintain the same firmware version on both CPs, and on both partitions of each CP. This organization enables you to evaluate firmware before you commit. As a standard practice, do not run mixed firmware levels on CPs.

Testing different firmware versions on Backbones

1. Connect to the Brocade Backbone IP address.
2. Enter the **ipAddrShow** command and note the address of CP0 and CP1.
3. Enter the **haShow** command and note which CP is active and which CP is standby. Verify that both CPs are in sync.
4. Enter the **firmwareShow** command and confirm that the current firmware on both partitions on both CPs is listed as expected.
5. Exit the session.
6. Update the firmware on the standby CP.

    a)   Connect to the Backbone and log in as admin to the standby CP.

    b)   Enter the **firmwareDownload -s** command and respond to the prompts.

           At this point, the firmware downloads to the standby CP only. When it has completed the download to that CP, reboot it. The current Backbone session is disconnected.

7. Fail over to the standby CP.

    a)   Connect to the Backbone on the active CP.

    b)   Enter the **haShow** command to verify that HA synchronization is complete. It takes a minute or two for the standby CP to reboot and synchronize with the active CP.

    c)   Enter the **firmwareShow** command to confirm that the primary partition of the standby CP contains the new firmware.

    d)   Enter the **haFailover** command. The active CP reboots and the current Backbone session is disconnected.

           If an AP blade is present : At the point of the failover, an *autoleveling* process is activated. Refer to Backbone firmware download process overview on page 29 for details about autoleveling.

8. Verify the failover.

    a)   Connect to the Backbone on the active CP, which is the former standby CP.

    b)   Enter the **haShow** command to verify that the HA synchronization is complete. It takes a minute or two for the standby CP, which is the old active CP, to reboot and synchronize with the active CP.

    NOTE
    If the CPs fail to synchronize, you can still proceed because the version being tested is already present on the active CP, and subsequent steps ensure that the standby CP is updated to the same version as the active CP.

    c)   Confirm the evaluation version of firmware is now running on the active CP by entering the **firmwareShow** command.

9. Update firmware on the standby CP.

    a)   Connect to the Backbone on the standby CP, which is the former active CP.

    b)   Enter the **firmwareDownload** command with the **-s -b -n** operands. This ensures that the following steps are successful.

At this point the firmware downloads to the standby CP only and reboots it. The current Backbone session is disconnected.

c) Wait one minute for the standby CP to reboot, and then connect to the Backbone and log in as admin.

d) Enter the **firmwareShow** command to confirm that *both* primary partitions have the test drive firmware in place.

You are now ready to evaluate the new version of firmware.

ATTENTION

Stop! If you want to *restore* the firmware, stop here and skip ahead to step 12; otherwise, continue to step 10 to commit the firmware on both CPs, which completes the firmware download.

---

10 Perform a commit on the standby CP.

From the current Backbone session on the standby CP, enter the **firmwareCommit** command to update the secondary partition with new firmware. It takes several minutes to complete the commit operation. Do not do anything on the Backbone while this operation is in process.

11 Perform a commit on the active CP.

a) From the current Backbone session on the active CP, enter the **firmwareShow** command and confirm that only the active CP secondary partition contains the old firmware.

b) Enter the **firmwareCommit** command to update the secondary partition with the new firmware. It takes several minutes to complete the commit operation. Do not do anything on the Backbone while this operation is in process.

c) Upon completion of the **firmwareCommit** command, enter the **firmwareShow** command to confirm both partitions on both CPs contain the new firmware.

d) Enter the **haShow** command to confirm that the HA state is in sync.

ATTENTION

Stop! If you have completed step 11, then you have committed the firmware on both CPs and you have completed the firmware download procedure.

---

12 Restore the firmware on the standby CP.

In the current Backbone session for the standby CP, enter the **firmwareRestore** command. The standby CP reboots and the current Backbone session ends. Both partitions have the same Fabric OS after several minutes.

13 Perform **haFailover** on the active CP.

a) In the current Backbone session for the active CP, enter the **haShow** command to verify that HA synchronization is complete. It takes a minute or two for the standby CP to reboot and synchronize with the active CP.

b) Enter the **haFailover** command. The active CP reboots and the current Backbone session ends. The Backbone is now running the original firmware.

14 Restore firmware on the "new" standby CP.

a) Wait one minute and connect to the Backbone on the new standby CP, which is the former active CP.

b) Enter the **firmwareRestore** command. The standby CP reboots and the current Backbone session ends. Both partitions have the same Fabric OS after several minutes.

c) Wait five minutes and log in to the Backbone. Enter the **firmwareShow** command and verify that all partitions have the original firmware.

If an AP blade is present : Blade partitions always contain the same version of the firmware on both partitions. The firmware is stored on the blade's compact flash card and is always synchronized with the active CP's firmware. Thus, if you restore the active CP firmware, the blade firmware is automatically downloaded (autoleveled) to become consistent with the new CP firmware (the blade firmware is restored).

Your system is now restored to the original partitions on both CPs. Make sure that servers using the fabric can access their storage devices.

If you want to upgrade a Backbone with only one CP in it, follow the procedures in Testing and restoring firmware on switches on page 33. Be aware that upgrading a Backbone with only one CP is disruptive to switch traffic.

Validating a firmware download

Validate the firmware download by running the following commands: **firmwareShow** , **firmwareDownloadStatus** , **nsShow** , **nsAllShow** , and **fabricShow**. Also, verify that no ports come up as G_Ports using the **switchShow** command.

All of the connected servers, storage devices, and switches should be present in the output of these commands. If there is a discrepancy, it is possible that a device or switch cannot connect to the fabric and further troubleshooting is necessary.

TABLE 3   Commands used for validating a firmware download

Command	Description
firmwareShow	Displays the current firmware level on the switch. For Brocade Backbones, this command displays the firmware loaded on both partitions (primary and secondary) for both CPs and AP blades. Brocade recommends that you maintain the same firmware level on both partitions of each CP within the Brocade Backbone. The **firmwareShow** command displays the firmware version on each CP.
firmwareDownloadStatus	Displays an event log that records the progress and status of events during Fabric OS, SAS, and SA firmware download. The event log is created by the current **firmwareDownload** command and is kept until another **firmwareDownload** command is issued. There is a time stamp associated with each event. When downloading SAS or SA in systems with two control processor (CP) cards, you can only run this command on the active CP. When downloading Fabric OS, the event logs in the two CPs are synchronized. This command can be run from either CP.
nsShow	Displays all devices directly connected to the switch that have logged in to the name server. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.
nsAllShow	Displays all devices connected to a fabric. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.
fabricShow	Displays all switches in a fabric. Make sure the number of switches in the fabric after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

Index

A

auto-leveling, FR4-18i blade 29, 35

B

Backbone
    upgrading firmware 29
Backbone firmware
    download 29
    download process overview 29
    version testing 34
blade
    upgrading firmware 29
Brocade DCX
    auto-leveling 17
Brocade DCX 8510
    auto-leveling 17
Brocade fixed-port switches, upgrading firmware 28

C

command
    configUpload 25
    errClear 25
    fabricShow
        described 37
    firmwareCommit 29, 33–35
    firmwareDownload 17, 20, 21, 25, 27–29, 31, 33
    firmwareDownloadStatus 27, 37
    firmwareRestore 33, 34
    firmwareShow
        described 37
    haFailover 35
    haShow 29, 35
    haSyncStart 29
    mapsconfig
        --enablemaps 13
    nsAllShow
        described 37
    nsShow
        described 37
    sshutil 20
    usbStorage 32
configUpload command 25
considerations

downgrading 13
    upgrading 11
CP 13
    See also Command Processor

D

downgrade considerations 13
downgrading firmware 14, 19

E

errClear command 25

F

Fabric Performance Impact monitoring 11
fabricShow command
    described 37
FICON CUP environment considerations 21
firmware
    Backbone 29
    Backbone download process overview 29
    Backbone version testing 34
    downgrading 19
    downloading without a password 20
    download process 17
    finding version 26
    for switches 27, 28
    obtaining and decompressing 25
    switch version testing 33
    upgrading 19
    upgrading for Brocade fixed-port switches 28
    upgrading on Backbones 29
    upgrading on blades 29
firmwareCommit command 29, 33–35
firmware downgrade considerations 14
firmware download